



UNITED
STATES
SECRET
SERVICE

counter threats to financial payment systems



**Office of
Investigations**
*Priorities and
Roadmap*

support protective responsibilities



strengthen and grow the workforce



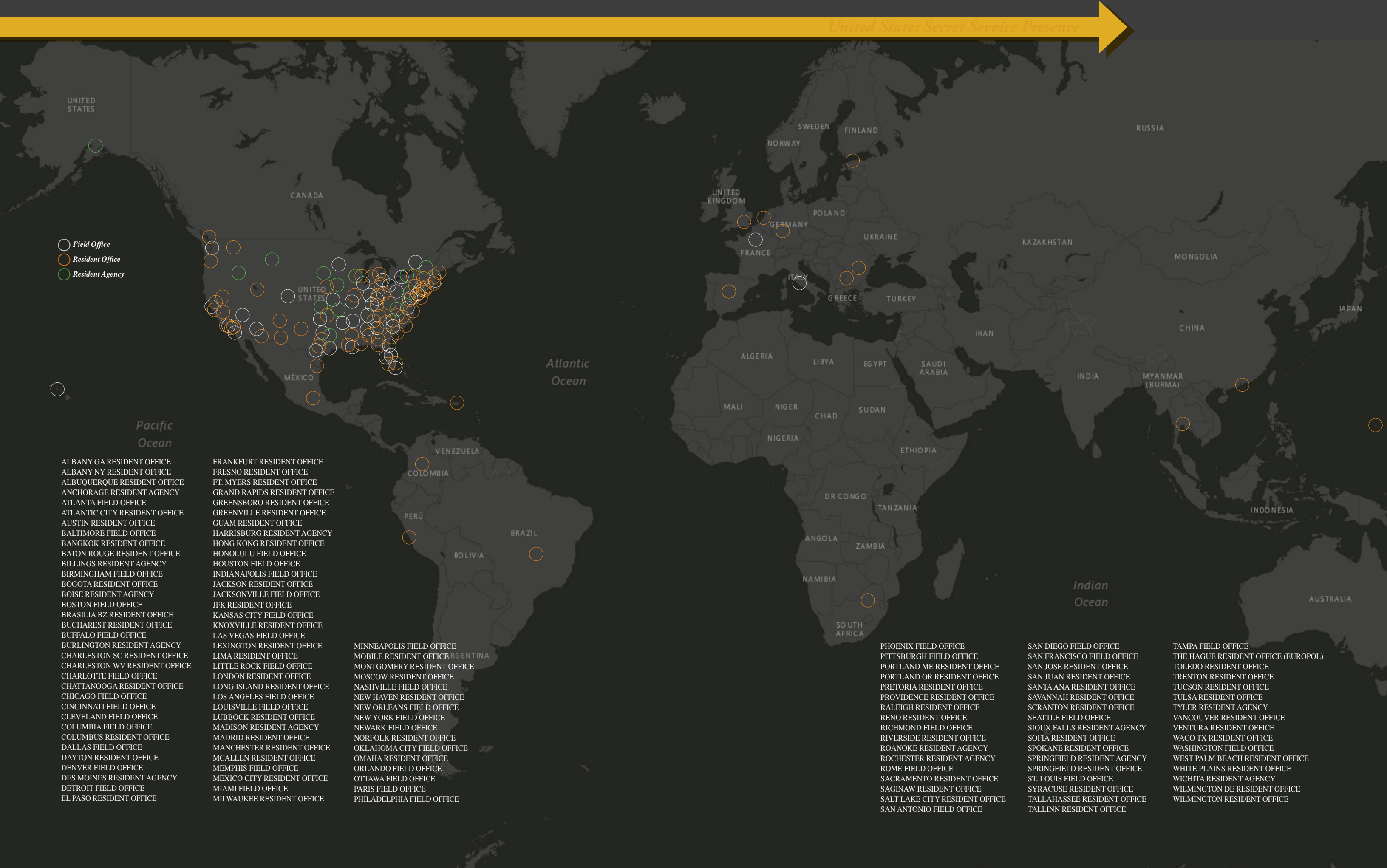
U.S. Department of
Homeland Security
**United States
Secret Service**



U.S. Department of
Homeland Security
**United States
Secret Service**

Office *of*
Investigations
Priorities and
Roadmap





- Field Office
- Resident Office
- Resident Agency

ALBANY GA RESIDENT OFFICE
ALBANY NY RESIDENT OFFICE
ALBUQUERQUE RESIDENT OFFICE
ANCHORAGE RESIDENT AGENCY
ATLANTA FIELD OFFICE
ATLANTIC CITY RESIDENT OFFICE
AUSTIN RESIDENT OFFICE
BATON ROUGE RESIDENT OFFICE
BILLINGS RESIDENT AGENCY
BIRMINGHAM FIELD OFFICE
BOGOTA RESIDENT OFFICE
BOISE RESIDENT AGENCY
BOSTON FIELD OFFICE
BRASILIA BZ RESIDENT OFFICE
BUCHAREST RESIDENT OFFICE
BUFFALO FIELD OFFICE
BURLINGTON RESIDENT AGENCY
CHARLESTON SC RESIDENT OFFICE
CHARLESTON WV RESIDENT OFFICE
CHARLOTTE FIELD OFFICE
CHATTANOOGA RESIDENT OFFICE
CHICAGO FIELD OFFICE
CINCINNATI FIELD OFFICE
CLEVELAND FIELD OFFICE
COLUMBIA FIELD OFFICE
COLUMBUS RESIDENT OFFICE
DALLAS FIELD OFFICE
DAYTON RESIDENT OFFICE
DENVER FIELD OFFICE
DES MOINES RESIDENT AGENCY
DETROIT FIELD OFFICE
EL PASO RESIDENT OFFICE

FRANKFURT RESIDENT OFFICE
FRESNO RESIDENT OFFICE
FT. MYERS RESIDENT OFFICE
GRAND RAPIDS RESIDENT OFFICE
GREENSBORO RESIDENT OFFICE
GREENVILLE RESIDENT OFFICE
GUAM RESIDENT OFFICE
HARRISBURG RESIDENT AGENCY
HONG KONG RESIDENT OFFICE
HONOLULU FIELD OFFICE
HOUSTON FIELD OFFICE
INDIANAPOLIS FIELD OFFICE
JACKSON RESIDENT OFFICE
JACKSONVILLE FIELD OFFICE
JFK RESIDENT OFFICE
KANSAS CITY FIELD OFFICE
KNOXVILLE RESIDENT OFFICE
LAS VEGAS FIELD OFFICE
LEXINGTON RESIDENT OFFICE
LIMA RESIDENT OFFICE
LITTLE ROCK FIELD OFFICE
LONDON RESIDENT OFFICE
LONG ISLAND RESIDENT OFFICE
LOS ANGELES FIELD OFFICE
LOUISVILLE FIELD OFFICE
LUBBOCK RESIDENT OFFICE
MADISON RESIDENT AGENCY
MADRID RESIDENT OFFICE
MANCHESTER RESIDENT OFFICE
MCALLEN RESIDENT OFFICE
MEMPHIS FIELD OFFICE
MEXICO CITY RESIDENT OFFICE
MIAMI FIELD OFFICE
MILWAUKEE RESIDENT OFFICE

MINNEAPOLIS FIELD OFFICE
MOBILE RESIDENT OFFICE
MONTGOMERY RESIDENT OFFICE
MOSCOW RESIDENT OFFICE
NASHVILLE FIELD OFFICE
NEW HAVEN RESIDENT OFFICE
NEW ORLEANS FIELD OFFICE
NEW YORK FIELD OFFICE
NEWARK FIELD OFFICE
NORFOLK RESIDENT OFFICE
OKLAHOMA CITY FIELD OFFICE
OMAHA RESIDENT OFFICE
OMAHA RESIDENT OFFICE
ORLANDO FIELD OFFICE
OTTAWA FIELD OFFICE
PARIS FIELD OFFICE
PHILADELPHIA FIELD OFFICE

PHOENIX FIELD OFFICE
PITTSBURGH FIELD OFFICE
PORTLAND ME RESIDENT OFFICE
PORTLAND OR RESIDENT OFFICE
PRETORIA RESIDENT OFFICE
PROVIDENCE RESIDENT OFFICE
RALEIGH RESIDENT OFFICE
RENO RESIDENT OFFICE
RICHMOND FIELD OFFICE
RIVERSIDE RESIDENT OFFICE
ROANOKE RESIDENT AGENCY
ROCHESTER RESIDENT AGENCY
ROME FIELD OFFICE
SACRAMENTO RESIDENT OFFICE
SAGINAW RESIDENT OFFICE
SALT LAKE CITY RESIDENT OFFICE
SAN ANTONIO FIELD OFFICE

SAN DIEGO FIELD OFFICE
SAN FRANCISCO FIELD OFFICE
SAN JOSE RESIDENT OFFICE
SAN JUAN RESIDENT OFFICE
SANTA ANA RESIDENT OFFICE
SAVANNAH RESIDENT OFFICE
SCRANTON RESIDENT OFFICE
SEATTLE FIELD OFFICE
SIOUX FALLS RESIDENT AGENCY
SOFIA RESIDENT OFFICE
SPOKANE RESIDENT OFFICE
SPRINGFIELD RESIDENT AGENCY
SPRINGFIELD RESIDENT OFFICE
ST. LOUIS FIELD OFFICE
SYRACUSE RESIDENT OFFICE
TALLAHASSEE RESIDENT OFFICE
TALLINN RESIDENT OFFICE

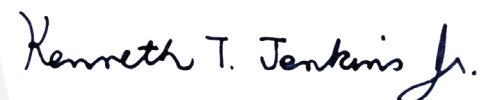
TAMPA FIELD OFFICE
THE HAGUE RESIDENT OFFICE (EUROPOL)
TOLEDO RESIDENT OFFICE
TRENTON RESIDENT OFFICE
TUCSON RESIDENT OFFICE
TULSA RESIDENT OFFICE
TYLER RESIDENT AGENCY
VANCOUVER RESIDENT OFFICE
VENTURA RESIDENT OFFICE
WACO TX RESIDENT OFFICE
WASHINGTON FIELD OFFICE
WEST PALM BEACH RESIDENT OFFICE
WHITE PLAINS RESIDENT OFFICE
WICHITA RESIDENT AGENCY
WILMINGTON DE RESIDENT OFFICE
WILMINGTON RESIDENT OFFICE

Note from the Assistant Director

The Secret Service is one of the nation’s oldest law enforcement agencies. Its founding mission is to investigate and counter threats to the financial payment systems of the United States. Since 1865, the Nation has regularly looked to the Secret Service to accomplish critical and challenging tasks.

The Office of Investigations is at the forefront of the execution of our integrated mission as the agency’s largest office. It has oversight of all field offices of the Secret Service, both domestic and international. The Office of Investigations continues to achieve notable results in the Secret Service’s founding mission. It suppresses counterfeit currency, addresses emergent threats, thwarts criminal enterprises in cyber crime and identity theft, even as we meet increasing protective requirements.

These results demonstrate the dedication and talent of Secret Service personnel, who are known for their pragmatic and relentless focus on accomplishing the mission, no matter the challenges before them. This *Investigative Priorities and Roadmap (Roadmap)* assesses the challenging operating environment we face and provides clear focus areas and strategies for the Office of Investigations. This *Roadmap* also informs our partners of our priorities, so that we can identify shared objectives and complementary efforts.



Kenneth Jenkins
Assistant Director
Office of Investigations

Executive Summary	1
I. Introduction	3
II. Operating Context	5
The Operational Environment.....	5
Role of U.S. Financial and Payment Systems Globally	5
Necessity of International Cooperation	5
Ongoing Digitization of Financial and Payment Systems	6
Growth of Digital Currencies	6
The Impact of Cyberspace on Criminal Investigations.....	7
Criminal Threats & Risks to U.S. Financial & Payment Systems.....	7
Increasing Cybersecurity Risks to Protectees and Critical Infrastructure	8
Integration with the Department of Homeland Security	9
Delivering Results in a Constrained Budget Environment.....	9
III. Focus Areas	11
1. Counter the most significant criminal threats to the financial and payment systems of the U.S.	11
2. Support protective responsibilities.....	12
3. Strengthen and grow the Secret Service workforce	13
IV. Conclusion.....	15

The Secret Service faces a range of challenges in accomplishing its responsibilities and continuing a more than 150-year tradition of excellence. Fiscal constraints require that the agency prioritize its efforts to address an evolving and global financial and payment system, as well as fulfilling its growing protective assignments. This *Investigative Priorities and Roadmap (Roadmap)* assesses these challenges. It provides clear strategies and milestones that address focus areas for the Office of Investigations.

The U.S. dollar is the world's foremost reserve currency. Its strength is partially due to the work of the Secret Service in investigating its counterfeiting and criminal exploitation. However, the financial system is currently in a period of innovation; it has long been at the forefront of adopting computers, and now this ongoing digitization is resulting in novel monetary instruments like Bitcoin and other digital currencies. This exposes U.S. financial institutions to global cybersecurity threats. Similar cybersecurity threats are increasingly presenting risk to Secret Service protectees, requiring the Secret Service to continue to leverage its investigative expertise in conducting its protective operations.

Budgetary constraints are likely to continue to be a challenge. As a result of sequestration, the Secret Service suspended most of its hiring from 2012 to 2014, and our budget declined from 2008 to 2013. While this trend has recently been reversed, it will take years to grow the Secret Service's workforce to meet current protective requirements. Quickly addressing this workforce gap is a critical priority.

To address these and other challenges, the Office of Investigations will prioritize efforts in the following three focus areas:

1. **Counter the most significant criminal threats to the financial and payment systems of the United States through criminal investigations.**
2. **Support protective responsibilities through investigation of threats and safeguarding the persons, locations, and events protected by the Secret Service.**
3. **Strengthen and grow the Secret Service workforce through identifying and developing the best personnel.**

This *Roadmap* will be implemented over the course of the next two years and synchronized with the federal budget process to ensure alignment of resource requests. Successful execution will require the Secret Service to continue to closely collaborate with our full range of partners, both government and non-government. Through these partnerships, the Secret Service is able to maximize its impact and achieve results disproportionate to the size of the agency.

Objectives of the Office of Investigations

1. **Counter the most significant criminal threats to the financial and payment systems of the United States through criminal investigations.**

Outcome: Reduce criminal activity against the US financial and payment systems through investigation and arrest of the most significant criminal threats.

2. **Support protective responsibilities through investigation of threats and safeguarding the persons, locations, and events protected by the Secret Service.**

Outcome: Office of Investigations supports 100% of protective requirements in a timely and efficient manner, conducts timely and thorough investigation of threats to our protectees, and secures critical infrastructure against potential threats to minimize risk to persons, facilities, and events protected by the Secret Service.

3. **Strengthen and grow the Secret Service workforce through identifying and developing the best personnel.**

Outcome: Ensure timely and effective recruiting and vetting of applicants and develop a workforce that is trained and equipped to perform the mission of the Secret Service. Reduce recruiting and vetting time to increase the number of hires with the necessary technical and investigative skills to perform the mission.



The Secret Service has a long history of safeguarding financial and payment systems from criminal exploitation. In 1865, the threat we were founded to address was that of counterfeit currency. As our financial payment systems have evolved, from paper to plastic to, now, digital information, so too has our investigative responsibilities. The Secret Service has a rich history of continual innovation in its approaches and methods to ensure it can accomplish its assigned responsibilities. This *Roadmap* continues this tradition by assessing the challenges the Secret Service must address and strategies and milestones that address focus areas for the Office of Investigations.

The Secret Service is assigned broad investigative jurisdiction to conduct law enforcement actions to safeguard financial and payment systems.¹ Global trust in financial and payment systems underpins economic prosperity and these systems are a critical enabler of global commerce. Safeguarding these systems from criminal exploitation is a critical responsibility of the Office of Investigations. The Secret Service must continue to accomplish these responsibilities in a constrained fiscal environment, even as we prioritize supporting the protective requirements, which have become the foremost responsibility of the Secret Service over the past 100 years.

Today, our modern financial system depends heavily on information technology for convenience and efficiency. Accordingly, criminals have adapted their methods and are increasingly using cyberspace to exploit our Nation's financial payment system by engaging in fraud and other illicit activities. Similarly, the Secret Service must continue to keep pace with innovation in financial and payment systems to ensure we are able to effectively perform our responsibilities. Since first being assigned investigative responsibility for computer crimes in 1984, the Secret Service has been a leader in investigating and countering cyber threats. Increasingly, the agency is applying this investigative expertise to ensure protected persons, facilities, and events are secure from cybersecurity threats. Similarly, the Office of Investigations must continually look to identify areas where the expertise it has developed for investigative purposes can be leveraged to advance our ability to perform our protective responsibilities.

The Secret Service has a rich history of accomplishing its mission through partnership with other law enforcement agencies and the private sector. For example, we have established a large network of Financial and Electronic Crimes Task Forces for this purpose. International partnerships are also increasingly vital to effectively counter the transnational criminal

networks that pose threats to the integrity of financial and payment systems. To be successful, the Secret Service must continue its tradition of accomplishing its mission through partnership with other organizations and agencies.

This *Roadmap* establishes clear strategies and milestones that address focus areas for the Office of Investigations, our field offices, and task forces. Further, this *Roadmap* guides our partnerships both domestically and internationally. This *Roadmap* will be reviewed and updated following each future publication of the Secret Service Strategic Plan.



¹ See 18 U.S.C. §§ 1028-1030 & 3056(b)

The Secret Service conducts its critical mission in an evolving operating environment impacted by several trends and factors. Particularly notable amongst these trends are: The ongoing innovation and adoption related to information and communications technologies; the growing significance of a wide range of transnational criminal activity; the continuing integration of the Secret Service with DHS; and, the challenging fiscal environment. Understanding these circumstances shapes how the Secret Service will prioritize and focus its efforts in executing our integrated mission.

The Operational Environment

Financial infrastructure and payment systems are globally trusted systems, underpinning economic prosperity and a source of strength for the United States. The integrity and trust in these systems depends upon the Secret Service continuing to safeguard them from all forms of criminal exploitation—from counterfeiting to money laundering to various forms of fraud. These systems are dynamic, subject to ongoing innovation and change in use, requiring the Secret Service to continually adapt to emerging trends in technology, design, and use of these systems.

Role of U.S. Financial and Payment Systems Globally

The U.S. dollar is the world’s foremost reserve currency, and most U.S. banknotes are held outside of the United States. Ten countries use the U.S. dollar as their official currency, and over fifteen other countries have substantially dollarized economies as a result of fixed exchange rates or the relative popularity and trust in U.S. currency compared to others. The global trust and use of U.S. currency is a source of economic strength for the United States but results in challenges that the Secret Service must overcome to combat criminal exploitation of U.S. financial and payment systems occurring in foreign countries.

Necessity of International Cooperation

The ever-changing progress of advanced technology and the Internet has created opportunities for transnational cyber criminals to remotely target the U.S. financial infrastructure and payment systems. Cyber crime trends related to major data breaches show increasing technical and operational sophistication and increasing financial impact. These crimes are increasingly transnational in nature and intertwine with the illicit use of computers. The transnational nature of cyber crime makes multilateral cooperation crucial. Countries must continue to collaborate against cyber criminals in a manner that provides for international legal consistency, lending itself to cohesive policy and integrated law enforcement efforts. Adopting a standardized legal framework for cyber crime is an important first step in multilateral collaboration. The USSS encourages foreign partners to adopt the Budapest Convention on

Cybercrime, and legal measures and processes consistent with its principles. The Budapest Convention, to which 54 countries have acceded and at least 15 countries are in the process of acceding to, lays a foundation for international cooperation related to cyber crime.

The transnational nature of cyberspace requires a greater degree of international law enforcement cooperation. It requires both international consistency with regards to relevant laws and the technical capability for international law enforcement entities to effectively collaborate and assist one another. One area of particular concern is evidence preservation and recovery. Harms from a criminal violation may occur in one country, devices used by a suspect exist in another country, and the suspect himself may reside in a third country. International efforts should continue to increase discussion and adoption of common practices surrounding cyber crime, along with increased operational collaboration and joint investigations.

Ongoing Digitization of Financial and Payment Systems

The U.S. financial sector continues to be at the forefront of adopting modern information and communications technology (ICT) to improve operations. In the 19th century, one of the major profitable uses of the early transatlantic telegraph cables was to facilitate trading between New York and London. Today, the market opportunities of accelerating movement of information by a few milliseconds is sufficient to finance multi-million dollar ICT infrastructure projects, such as laying new transatlantic fiber-optic cables. For the past fifty years, the U.S. financial sector has also been at the forefront of adopting and integrating computers into operations, which has resulted in new criminal risks to their operation. Financial payment systems face substantial cybersecurity risks, with industry estimates of hundreds of billions of dollars in financial losses from malicious cyber activity. Future innovations, such as artificial intelligence and quantum computing, have the potential to further change the nature of financial sector operations and increase both the capabilities of, and the risks to, financial and payment systems. The Secret Service must continue to keep pace with the systems it is responsible for safeguarding and securing, and ensure we remain able to safeguard those systems from criminal risks.

“The U.S. financial sector continues to be at the forefront of adopting modern information and communications technology (ICT) to improve their operations.”

Growth of Digital Currencies

Digital currencies² are creating new opportunities for criminals to engage in illicit activity as a means for money

² “Digital currency” means an alternative currency that is stored on and transferred through computer systems; it exhibits some properties similar to currencies that are legal tender of the United States or other countries and is used as a substitute for or converted to legal tender. Currently no digital currency serves as legal tender in the U.S. or any other country; as such digital currencies are a subset of virtual currencies as defined by current Financial Crimes Enforcement Network (FINCEN) guidance FIN-2013-G001 (issued March 18, 2013).

laundering and crypto-ransomware. Digital currencies also have potential to substantially disrupt the nature of financial and payment systems. The Secret Service has successfully investigated and apprehended the founders and operators of two centralized digital currencies, e-Gold and Liberty Reserve, effectively ending their operations. The growth of decentralized cryptocurrencies presents new challenges for law enforcement, requiring continued innovation in investigative techniques employed by the Secret Service.

The Impact of Cyberspace on Criminal Investigations

Modern information technology is substantially changing the work of law enforcement. Evidence in criminal investigations is often scattered across numerous domestic and international jurisdictions, and may be held by a wide range of technology providers and digital devices. Additionally, criminals are progressively using cyberspace to collaborate, form transnational criminal organizations, reach victims globally, and organize complex criminal schemes—all while maintaining their anonymity from each other and their victims. Accordingly, criminal investigations increasingly require teams of law enforcement investigators who have knowledge of computer forensics, digital investigations, and the tradecraft necessary to identify and collect evidence from the various information systems. The Secret Service must continue to be at the forefront of developing innovative investigative techniques and sharing these best practices across the law enforcement community.

Criminal Threats & Risks to U.S. Financial & Payment Systems

Financial gain continues to be a primary driver of the most sophisticated criminal schemes, and financial and payment systems are a common target of both domestic and transnational criminals. In FY 2017, Secret Service financial and cyber crime investigations prevented over \$3 billion in fraud losses. Counterfeiting continues to be a risk to the integrity of U.S. currency. In FY 2017, 0.0093% of U.S. currency in circulation was identified as counterfeit, with tens of millions in counterfeit U.S. currency passed annually both domestically and abroad. Identity theft and access device fraud, a criminal violation of 18 U.S.C. §§ 1028, 1028A, and/or 1029, plays a substantial and growing role in these and other criminal activities.

Empowered by information and communications technologies, criminals targeting U.S. financial and payment systems are increasingly operating as networks of transnational criminals. These criminal networks use various organizing structures and vary from having a core group located in the same city to globally dispersed networks that have never met in person. Regardless of their particular organizing structure and dispersion, their core members tend to be located in countries where there is limited law enforcement cooperation with the United States or a high

“In FY 2017, Secret Service financial and cyber crime investigations prevented over \$3 billion in fraud losses.”

degree of government corruption. Naturally, their dispersed network of associates typically use the language of this core group of members.

A critical component of the Secret Service’s work is to identify the most significant criminal networks, including associated facilitators, and then prioritize its efforts to counter and defeat them. Currently, the most significant transnational cyber crime networks are those that emerged from the former Soviet Union states in Eastern Europe. This network of Russian-speaking actors is relentlessly weakening global information security, stealing billions from U.S. organizations, manipulating equity markets, and has built and employed their own cyber attack capabilities. These criminal networks have greater capability to conduct cyber operations than most governments. Meanwhile, the most prolific producers of U.S. counterfeit currency has recently been a network of Spanish-speaking counterfeiters in South America. This group uses existing drug and illicit trafficking networks to smuggle their counterfeit notes into the United States.

Countering transnational criminal organizations continues to be a priority of the U.S. Government and the Secret Service. Through our persistence and effective partnership with foreign law enforcement, the Secret Service has arrested and extradited transnational criminals responsible for hundreds of millions of dollars in financial losses to U.S. businesses and the production of millions in counterfeit notes. On 9 February 2017, the President signed Executive Order 13773 on “Enforcing Federal Law with Respect to Transnational Criminal Organizations and Preventing International Trafficking.” This order emphasizes the need to “strengthen the enforcement of Federal law in order to thwart transnational criminal organizations and subsidiary organizations,” including those engaged in illicit activities related to corruption, cyber crime, fraud, financial crimes, and money laundering. The Secret Service is committed to executing this order and continuing to counter the most significant criminal threats to the integrity of financial and payment systems through close partnerships domestically and abroad.

Increasing Cybersecurity Risks to Protectees and Critical Infrastructure

Exploitation of information and communications technologies also presents new risks affecting the protective responsibilities of the Secret Service, as well as to the Nation’s critical infrastructure.

Malicious actors are increasingly using cyberspace to remotely disrupt critical services or damage infrastructure by malicious manipulation of control systems. Additionally, Secret Service must be able to detect and counter a variety of emergent technology risks, from remotely or autonomously operated vehicles to new surveillance techniques. Often,

“Malicious actors are increasingly using cyberspace to remotely disrupt critical services or damage infrastructure by malicious manipulation of control systems.”

sophisticated cyber actors employ techniques similar to those used by cyber criminals in the pursuit of political or national security objectives, sometimes even using the same illicit cyber crime services. This provides the Secret Service an outstanding opportunity to apply our investigative expertise in executing our protective responsibilities.

Integration with the Department of Homeland Security

The Department of Homeland Security executes the critical mission of safeguarding the American people, the U.S. homeland, and American values. When it was created, it consolidated a range of government agencies with related responsibilities, including the Secret Service and most of the law enforcement personnel assigned to the Department of Treasury. While the Department of Treasury remains a critical partner,³ the Secret Service supports the Secretary of Homeland Security in the performance of departmental responsibilities through unity of effort across the entire homeland security enterprise.

The Secret Service performs a substantial role in executing three of the goals specified in the 2014 Quadrennial Homeland Security Review and FY 2014-2018 DHS Strategic Plan:

- Goal 1.3: Reduce Risk to the Nation’s Critical Infrastructure, Key Leadership, and Events.
- Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations and Other Illicit Actors.
- Goal 4.3: Advance Law Enforcement, Incident Response, and Reporting Capabilities.

Additionally, the Secret Service assists partners across the homeland security enterprise, based upon our unique expertise, to counter terrorism, child exploitation, and other significant criminal threats. Accordingly, the Secret Service must continue to strengthen its partnerships across DHS in order to achieve shared goals and objectives.

Delivering Results in a Constrained Budget Environment

Since 2010, the Federal government has operated under multiple continuing resolutions instead of regular appropriations. Although the continuing resolutions allow for agencies to continue operating, they do so in a more restricted manner than under regular appropriations. Additionally, sequestration, which went into effect in 2013, reduces resources and creates management challenges for the Secret Service in achieving its goals. The Secret Service’s budget declined, in real terms, from 2008 to 2013. While this trend was reversed in the FY 2014-2017 budgets, the previous decline resulted in a substantially reduced workforce as the Secret Service entered the 2016 campaign. Meanwhile, the protective requirements of the Secret Service have continued to grow, compounded by the long-term trend of increased

protectee travel, to include international travel, and the additional security efforts required to counter the modern terrorist threat.

To be successful in this challenging environment, the Secret Service must prioritize its activities to focus on delivering results. The agency must identify areas to improve efficiency and to prudently accept some risks to ensure success in performing critical missions. Additionally, the Secret Service must continue to develop its workforce, ensuring that it is building teams of special agents and professional staff that have the necessary mix of investigative, technological, and cultural skills to counter technologically advanced transnational threats.



³ Among other responsibilities, the Department of Treasury oversees the design of U.S. Currency, operates the Financial Crimes Enforcement Network (FINCEN), and is the Sector Specific Agency for Financial Services.

The Office of Investigations will prioritize its efforts to meet the challenges posed by the current operating environment. It will continue the Secret Service's tradition of excellence as we maintain the full trust and confidence of the nation. The following focus areas are the priorities for the Office of Investigations. Our efforts will focus on achieving these outcomes and improving our efficiency and effectiveness in support of them.

1. Counter the most significant criminal threats to the financial and payment systems of the United States through criminal investigations.

The investigative responsibilities of the Secret Service have gradually expanded to keep pace with the changing nature of financial and payment systems and allow us to effectively safeguard these systems. Meanwhile, the importance and complexity of executing this responsibility has grown as the financial and payment systems of the United States have become increasingly globally trusted, underpinning substantial economic activity world-wide. Accordingly, to effectively safeguard these systems the Secret Service must focus its investigative efforts on the following priority threats:

- i) Criminal activity with significant economic and financial impacts to the US;
- ii) Criminal activity, such as cybersecurity threats, that operate at scale and present emergent or systemic risks to financial and payment systems; and,
- iii) Transnational criminal activity involving corruption, illicit finance, fraud, money laundering, and other financial crimes.

To counter these threats, the Office of Investigations partners across the homeland security enterprise to maximize the impact of its investigative activities through increased investigations of high-impact criminal activity. The Secret Service will counter transnational criminal networks by operating as an integrated network of investigative teams, where investigative activities spanning multiple Secret Service field offices combine the skillsets of a diverse set of criminal investigators, analysts, and other relevant experts. The Secret Service will strengthen its existing task forces while aligning enterprise-wide investigative activities from independent or uncoordinated cases into a systematic, well-prioritized, and targeted operation to counter the networks of transnational criminals that present risks to financial and payment systems. This will be accomplished by:

- A) Expanding investigative purview to develop intelligence to holistically assess risks, detect and identify significant criminal activity, and target and prioritize investigative activities.

- B) Conducting high-impact investigations to suppress and counter these activities and seize illicit assets, and reconstitute victims of these crimes.
- C) Strengthening and expanding our network of Electronic and Financial Crimes Task Forces.
- D) Developing effective investigative teams with specialized expertise.
- E) Increasing collaboration amongst field offices and headquarters to address increasingly global and networked nature of criminal threats.
- F) Developing the capabilities of our law enforcement partners to aid us in countering key criminal threats.
- G) Fostering partnership with academia and private organizations to counter emergent criminal techniques and assist them in countering other significant criminal activity, such as child exploitation and terrorism.
- H) Rapidly developing and employing techniques and technologies to keep pace with changes to both criminal activities and the financial and payment systems we safeguard.
- I) Provide training to key foreign partners in investigative techniques, to include techniques for investigating cyber crime.

Outcome: Reduce criminal activity against the U.S. financial and payment systems through investigation and arrest of the most significant criminal threats.

2. Support protective responsibilities through investigation of threats and safeguarding the persons, locations, and events protected by the Secret Service.

The foremost responsibility of the Secret Service is to ensure effective performance of our protective responsibilities. The Office of Investigations substantially and routinely supports protective requirements and must ensure that we continue to provide timely and effective support.

The Office of Investigations also provides critical support to protective operations by applying its expertise to counter emergent risks. The Secret Service performs this on a daily basis to mitigate cybersecurity risks for the President and Vice President. In addition, the Secret Service partners with DHS components, State and Local law enforcement, and the private sector to develop and implement a comprehensive operational security plan for special security events. Secret Service agents trained and experienced in investigating cyber crime apply these skills to accomplish protective responsibilities. Cybersecurity efforts are coupled with the physical protection tactics allowing the Secret Service to maintain full control over both the cyber and physical environments in executing our protective responsibilities.

As such, it is imperative that the Secret Service proactively identify and mitigate the risks posed by malicious cyber actors to our protected persons, facilities, and events. Additionally, the Secret Service must leverage its unique expertise and experience to support broader homeland security objectives and secure critical infrastructure from cybersecurity risks.

In support of the protective responsibilities of the Secret Service the Office of Investigations will:

- A) Apply investigative expertise to counter emergent protective risks, such as those related to cybersecurity and remotely operated systems.
- B) Support the Office of Strategic Intelligence and Information with timely and thorough investigations of threats to our protectees.
- C) Support the Office of Protective Operations by providing personnel to support protective security plans.
- D) Collaborate with key foreign partners in dignitary protection by providing guidance and insight as it pertains to both physical and cybersecurity measures.

Outcome: Office of Investigations supports 100% of protective requirements in a timely and efficient manner, conducts timely and thorough investigation of threats to our protectees, and secures critical infrastructure against potential threats to minimize risk to persons, facilities, and events protected by the Secret Service.

3. Strengthen and grow the Secret Service workforce through identifying and developing the best personnel.

The success of the Secret Service depends on maintaining the most capable and trusted workforce. The Office of Investigations performs a critical role in supporting the Secret Service by: identifying, recruiting, and vetting the future employees of the Secret Service; supporting its personnel by providing them the continuing training, equipment, guidance, and experience they require to effectively perform the mission of the Secret Service; and ensuring it is retaining and continually developing the specialized expertise essential to our mission.

To support the continued success of the Secret Service, the Office of Investigations will:

- A) Train, equip, and provide developmental opportunities to its personnel to ensure they are best prepared to contribute to the success of the Secret Service.
- B) Retain and continually develop the specialized expertise essential to the mission of the Secret Service.
- C) Support the Office of Human Resources by identifying, recruiting, and vetting potential future employees.

- D) Partner with the Office of Training to ensure training is aligned to prepare Secret Service personnel to join our field offices and effectively perform their responsibilities.

Outcome: Ensure timely and effective recruiting and vetting of applicants and develop a workforce that is trained and equipped to perform the mission of the Secret Service. Reduce recruiting and vetting time to increase the number of hires with the necessary technical and investigative skills to perform the mission.



This *Investigative Priorities and Roadmap (Roadmap)* provides clear objectives to focus and prioritize our activities and ensure the Secret Service's continued success in accomplishing its integrated mission. The Secret Service does not execute its mission alone, but rather through partnership with other agencies and organizations. As such, this *Roadmap* also serves to clearly communicate to current and potential partners our mission and focus so that we can identify shared interests and opportunities for collaboration. Over the coming years, as the Office of Investigations implements this *Roadmap* and aligns its efforts to these focus areas, the Secret Service will remain an adaptive and innovative organization, ready to react to emerging threats and adjust our efforts based on a pragmatic assessment of effectiveness and efficiency. By prioritizing and focusing our efforts to achieve maximum impact, we can continue to demonstrate excellence in performing our mission.

